UNITED STATES DISTRICT COURT

for the

Eastern District of Tennessee

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
RESIDENTIAL PROPERTY LOCATED AT 8526 SHACKLEFORD LANE, STRAWBERRY PLAINS, TN 37871-1008

Case No. 3:19-MJ-2018

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Tennessee
(identify the person or describe the property to be searched and give its location):
Residential property located at 8526 Shackleford Lane, Strawberry Plains, TN37871-1008. Photographs and property descriptions are attached hereto as Attachment A and fully incorporated herein.

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:
See Attachment B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before February 21, 2019
(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge H. Bruce Guyton.
(name)

I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* for _____ days *(not to exceed 30)*.

☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 2-7-19 at 3:15pm Bruce Guyton
Judge's signature

City and state: Knoxville, Tennessee H. Bruce Guyton, U.S. Magistrate Judge
Printed name and title

Return

Case No.: 3:19-MJ-2018	Date and time warrant executed: 02/08/2019 0700hrs	Copy of warrant and inventory left with: Shawne Huff

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

1 Crucial SSD Drive (S/N: 1542F00E9A04)

1 Hitachi Hard Drive (S/N: F326GBRD)

1 Samsung Galaxy (IMEI: 355217091651605) w/ 32GB micro SD card

AND Electronic contents of the following:

1 iPhone registered to Shawne Huff

1 HP Silver Probook 450 G4 Laptop (S/N: 5CD7469 3MY)

6 Flash drives (2 Sandisk, 2 Lexar, 2 unlabeled) found in basement bedroom

6 unlabeled Flash drives in Benton Phillips' backpack

FEB 08 2019

Clerk, U. S. District Court
Eastern District of Tennessee
At Knoxville

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 02/08/2019

Executing officer's signature

Sean Wilson, Special Agent

Printed name and title

ATTACHMENT A

PROPERTY TO BE SEARCHED

The property to be searched is residential property located at 8526 Shackleford Lane, Strawberry Plains, TN 37871-1008, further described as a two-story single family residence with mostly brick exterior, stone lined front stairs and entry, white siding, a gray roof, and a wooden deck to the left of the entry. The property is pictured below.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. All records, documents, programs, applications and information relating to violations of 18 U.S.C. § 115(a)(1)(B)—(Influencing Federal Official by Threat) and 18 U.S.C. § 875(c)—(Interstate Communication of Threat), (collectively, the "Subject Offenses"), including:

a. All records, documents, programs, applications, and information reflecting or relating to any intent, motive, or means of committing violations of the Subject Offenses;

b. All records, documents, programs, applications, and information reflecting any usernames, monikers, and social media and email accounts used to commit violations of the Subject Offenses;

c. All records, documents, programs, applications, and information reflecting the intent or capacity to harm any person or carry out any threats against any person or property;

d. Any and all records, books, magazines, videos, and related correspondence, in whatever form, including handwritten and computer-generated, pertaining to attacks on persons and/or property;

e. Any and all photographs of weapons, ammunition, Senators, Congressmen/Congresswomen, federal facilities, or residences of the foregoing;

f. Indicia of occupancy, residency, and/or ownership of the Premises to be searched;

g. Firearms and ammunition;

h. Electronic devices used to facilitate violations of the Subject Offenses, including but not limited to, computers, routers, modems, hard drives, flash drives, thumb drives, cell phones, tablets, printers, and label making devices;

i. Information and/or data stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer or with the aid of computer-related equipment that was used to facilitate violations of the Subject Offenses. This media includes floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser discs, video cassettes, and other media that is capable of storing magnetic coding, as well as punch cards, and/or paper tapes, and all printouts of stored data;

j. Electronic devices that are capable of analyzing, creating, displaying, converting or transmitting electronic or magnetic computer data that were used to facilitate violations of the Subject Offenses. These devices include computers, computer components, computer peripherals, word-processing equipment, modems, monitors, cables, printers, plotters, encryption circuit boards, optical scanners, external hard drives, external tape backup drives, and other computer-related electronic devices;

k. Any and all instructions or programs stored in the form of electronic or magnetic media that are capable of being interpreted by a computer or related components. The items to be seized include operating systems, application software, utility programs, compilers, interpreters and other programs or software used to communicate with computer hardware or peripherals either directly or indirectly via telephone lines, radio, or other means of transmission; and

l. Any and all written or printed material that provides instruction or examples concerning the operation of computer systems or software, and/or any related device, and sign-on passwords, encryption codes or other information needed to access the computer system and/or software programs.

2. With respect to any electronic device used to facilitate the violations of the Subject Offenses or containing evidence falling within the scope of the foregoing categories of items to be seized:

a. Evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, monikers, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

b. Evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. Evidence of the presence or absence of computer software, hardware, or other application, which allows for anonymization of usage on a computer device, including Tor, Virtual Private Networks, VMWare, VirtualBox, multiple boot capabilities, virtualization/virtual machine software, and drive cleaning/wiping software;

d. Evidence of the presence or absence of encryption software, hardware, or other application;

e. Any evidence of Internet research or communications regarding anonymization tools, encryption methods, virtual currency, and virtual currency trading platforms;

f. Any evidence of Internet searches or communications regarding the firearms and destructive devices, including any negotiations or purchases of such items;

g. Evidence of the attachment of other devices;

h. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

i. Evidence of the times the device was used;

j. Passwords, encryption keys, and other access devices that may be necessary to access the device;

k. Applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

l. Records of or information about Internet Protocol addresses used by the device; and

m. Records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

II. SEARCH PROCEDURE FOR ELECTRONIC DEVICES

1. In searching the electronic devices (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search any electronic device capable of being used to facilitate violations of the Subject Offenses or containing data falling within the scope of the items to be seized.

b. The search team will, in its discretion, either search each electronic device where it is currently located or transport it to an appropriate law enforcement laboratory or similar facility to be searched at that location. Members of the search team may also access the electronic devices remotely.

c. The search team shall complete the search of the electronic devices as soon as is practicable, but not to exceed 120 days from the date of issuance of the warrant. The government will not search the electronic device(s) beyond this 120-day period without first obtaining an extension of time order from the Court.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each electronic device capable of containing any of the items to be seized to the search protocols to determine whether the electronic device and any data therein falls within the scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

e. If the search team, while searching an electronic device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the search team shall immediately discontinue its search of that electronic device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

f. If the search team determines that an electronic device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the electronic device and delete or destroy all forensic copies thereof.

g. If the search team determines that an electronic device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

h. If the search team determines that the electronic device is (1) itself an item to be seized and/or (2) contains data falling within the list of items to be seized, the government may retain forensic copies of the electronic device, but may not access data

falling outside the scope of the items to be seized (after the time for searching the device has expired) absent further order of the Court.

i. The government may retain an electronic device itself until further order of the Court or one year after the conclusion of the criminal investigation or case, only if the electronic device is determined to be an instrumentality of an offense under investigation or the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the electronic device (or while an application for such an order is pending). Otherwise, the government must return the electronic device.

j. After the completion of the search of the electronic devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

2. The special procedures relating to electronic devices found in this warrant govern only the search of electronic devices pursuant to the authority conferred by this warrant and do not apply to any search of electronic devices pursuant to any other order of the Court.